UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WASHINGTON

RIVER CITY MEDIA, LLC, et al., Plaintiffs, v. KROMTECH ALLIANCE CORPORATION, et al., Defendants.	Case No. 2:17-cv-00105-SAB **DECLARATION OF MARK FERRIS IN SUPPORT OF PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS**

I, Mark Ferris, make the following declaration based upon my own personal knowledge and information provided to me by others at River City Media, LLC ("River City"):

Background on River City and Commercial Email Marketing

1. I am a Member of, and the Chief Technical Officer for, River City Media, LLC ("River City"). I reside in Idaho.

2. River City is a successful internet-based marketing company based in Eastern Washington.

3. Some of the world's most recognizable brands use River City to help market their products including MetLife, LifeLock, Liberty Mutual, Match.com, DirectTV, and Lyft.

NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

4. River City built its reputation on its consistent production of transparent, clean, and quality email marketing campaigns. River City has never been the subject of a federal or state investigation or lawsuit related to commercial email laws or regulations, nor has River City been sued by a private party for violations of the CAN-SPAM Act or other commercial email laws.

5. River City is a technology company focused entirely on internet marketing and commercial email. It depends on its technology, data, and relationships to survive and prosper. Most of River City's material is sensitive, private, and proprietary data that includes fine-tuned methodologies and technological know-how that River City considers to be its trade secrets.

6. In order to do business, River City must create or purchase massive databases of consumer email addresses for people who have opted-in to receive commercial email from advertisers and publishers.

7. River City also creates proprietary algorithms and techniques to conduct its email marketing campaigns lawfully and with full transparency and the highest quality. River City also maintains records for its partnerships and is expected to keep those records safe and secure.

8. I have worked in the online marketing industry for over a decade and am intimately familiar with what it takes to succeed in this industry. In my experience, a company's reputation is paramount to its ability to succeed. River City's reputation among marketing and advertising agencies and advertisers themselves is—or was—one of its most valuable assets.

9. River City's ability to carry out its basic business operations depends on relationships with dozens of third parties including internet access providers, Email Service Providers, affiliates, advertisers, and more.

Cyberattack on River City's Network

10. I initially became aware of a possible cyberattack (hacking campaign) against River City on or about January 15, 2017, when a database server was

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

compromised. By February 9, 2017, I realized that River City's network had been heavily compromised and that the January 15 attack was not just an isolated hack. Ultimately, this cyberattack proved designed to—and in fact did—cripple River City's infrastructure and destroy its reputation.

11. The attacker, revealed to be Chris Vickery by tweets and multiple news articles, methodically gained access to River City's network of computers and databases. Vickery was never authorized by me or anyone at River City to conduct his computer intrusions—River City did not hire him to conduct a security penetration test.

12. In fact, Vickery downloaded gigabytes of River City's data that he later shared with technology news bloggers and the public. Vickery publicly tweeted about his activities:

13. Once Vickery gained access to River City's network, he did not merely download and distribute River City's sensitive, confidential, and proprietary data—he also intentionally caused severe damage to River City's network infrastructure.

14. River City's employees and third-party technicians examined the results of Vickery's attack and concluded that Vickery sent targeted commands to River City's "netbox," a Linux-based server that provided a map (or "network topology") of River City's network. Vickery's commands deleted nearly every record in "netbox," effectively crippling River City's ability to manage its own

NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

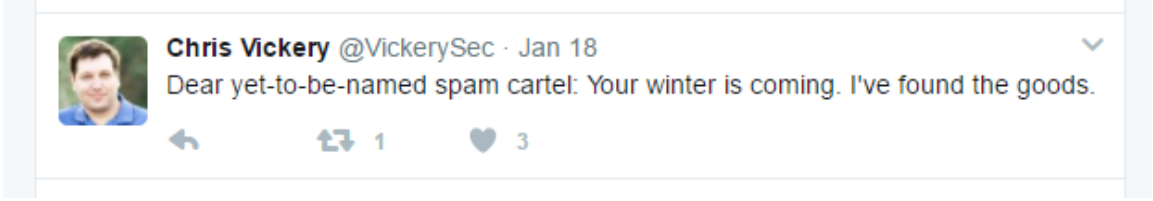
systems and conduct its normal business operations, let alone try to recover from Vickery's malicious assault.

15. A true and correct copy of command line logs for River City's computers is attached hereto as Exhibit 1 and shows Vickery searching through River City's network in a manner that only an intruder would use.

16. River City also discovered that Vickery used credentials (i.e. usernames and passwords) stored in the data he downloaded to access multiple third-party services used by River City in its business. Vickery logged into River City's PayPal account and purchased domain names from one of River City's domain registrars. Vickery accessed River City's company email accounts and company Hipchat servers and chat histories. He accessed and misused River City's Email Service Provider accounts (which is one method River City uses to send its lawful commercial emails). Vickery also logged into or accessed River City's affiliate network accounts and its GitHub account. These third-party services exist on servers and computers not owned by River City.

17. Vickery even used River City's Email Service Providers to send unlawful and offensive emails: appearing to come from one of River City's principals (Alvin Slocombe), the emails had the subject line "Donald Trump's Transvestite Surprise" and the body of the email contained the text, "Try and Stop Me Bitch." River City did not authorize these emails to be sent.

18. I later discovered that Vickery hinted at his successful attack: on January 18, 2017, Vickery tweeted that he had "found the goods":



The Media Campaign

NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

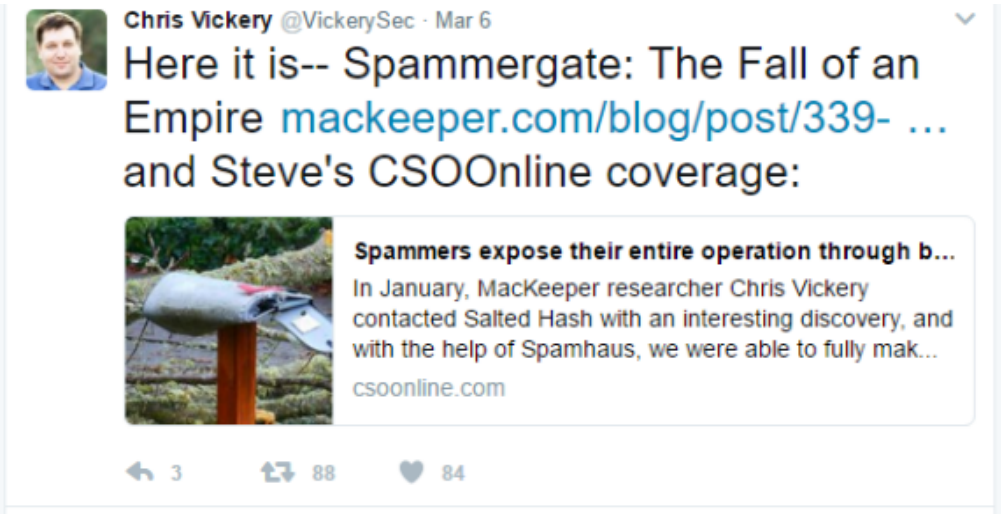
19. Vickery's March 3, 2017, "teaser tweet" references "@SteveD3," or Steve Ragan, a technology writer employed by CSOOnline.com, with whom Vickery shared River City's data; in this tweet, Vickery thanks Ragan for "cooperating on investigation."

20. Vickery and Steve Ragan published their articles on March 6, 2017, without ever attempting to contact River City beforehand. The articles were a surprise and caused the vast majority of the reputational damage upon being published.

21. A true and correct copy of Vickery's March 6, 2017, Mackeeper.com article, located at https://mackeeper.com/blog/post/339-spammergate-the-fall-of-an-empire is attached hereto as Exhibit 2.

22. A true and correct copy of Ragan's March 6, 2017, "Salted Hash" CSOonline.com article, located at http://www.csoonline.com/article/3176433/security/spammers-expose-their-entire-operation-through-bad-backups.html is attached hereto as Exhibit 3.

23. Vickery's March 6, 2017, tweet is a link to Ragan's story and Vickery's own blog at Mackeeper.com.



24. CSOonline.com calls itself the "leading source" for security professionals to "connect exclusively with key security decision-makers" and

boasts 786,000 average monthly page views from 395,000 average monthly unique visitors, according to the CSO Media Kit, posted online at https://www.idgenterprise.com/reach/cso/. A true and correct copy of the CSO Media Kit downloaded on April 28, 2017, is attached hereto as Exhibit 4.

25. Vickery then posted confidential information about River City's business operations to his Twitter feed:

26. Ragan included similar information from a file that contained company addresses in his follow-up story, posted on March 8, 2017, "SpammerGate: The takeaway lessons and follow-ups on the River City media data breach", available at http://www.csoonline.com/article/3178395/security/spammergate-the-takeaway-lessons-and-follow-ups-on-the-river-city-media-data-breach.html, last visited May 2, 2017, attached hereto as Exhibit 5:

NEWMAN DU WORS LLP
2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

3	Acme Media
4	Ad Media Plus
5	Bfons, LLC.
6	Blue Fences, LLC.
7	Books Of Wonders For Everyone Inc.
8	Brand 4 Marketing, LLC.
9	Click This, LLC.
10	CloudFly
11	Cloudspace Technologies
12	Cooperative Investments, LLC.
13	DogWorkDot Inc.
14	eBox
15	Fish&Chips
16	ForceNet, LLC.
17	Grow Clientele, LLC.
18	Halofish, LLC.
19	IR Media, LLC.
20	Its Technical, LLC.
21	Jasper Findings, LLC.
22	Jaxer Solutions
23	KN Media, LLC.
24	Klaur Technology
25	Luma Condominiums
26	MH Marketing, LLC.
27	Media5321, LLC.
28	Micromax Enterprises, LLC.
29	Pheasant Valley Marketing Group
30	RCM Delivery
31	RCM Idaho LLC.
32	River City Media, LLC.
33	Rylekor, LLC.
34	SAMIAM Inc.
35	Site Traffic Network
36	Slip7 Media, LLC.
37	Social Endeavors, LLC.
38	The Wishing Well Company
39	VR Endeavors, LLC.
40	[redacted]al Ad Group, LLC.
41	[redacted] Web Domains
42	Winston Dynamics, Inc.
43	Zero Systems, LLC.

Alternate business names used by River City Media

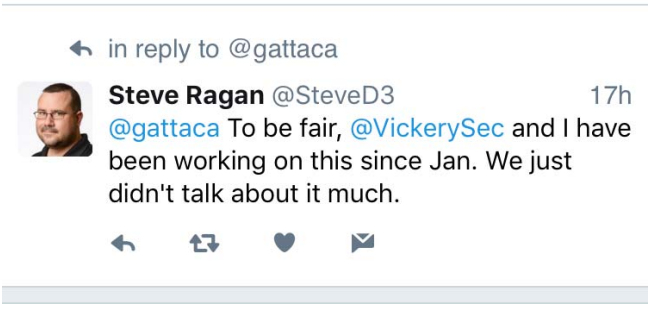
As a result of our story, one of the largest marketing firms working with RCM, Amobee, said the company was dropped from their affiliate service, AdDemand. However, this does nothing to prevent RCM and its staff from switching to a new alias and starting over. In fact, they're already attempting to switch aliases.

Late in the day on Monday, shortly after the story dropped, RCM employees started removing social media profiles and one switched her position from CEO of River City Media, to CEO of Slip7Media. The image to the left is a list of some of the aliases used by RCM, based on insurance documents and domain registrations.

Spamhaus added Domainers Choice (one of the registrars used by RCM) to the number two spot on the Top 10 list of abused domain registrars, the index currently shows that 99.4% of the domains registered there are bad.

27. Lists of corporate entities, domain names, and IP addressed used by email marketing companies are carefully kept secrets and necessary components of running a successful business in this industry. River City considers such data its trade secrets. Ragan and Vickery caused enormous damage to River City just by disclosing these lists.

28. Ragan later tweeted about his participation in Vickery's "investigation" saying, "To be fair, @VickerySec and I have been working on this since Jan. We just didn't talk much about it much."



29. Ragan and Vickery obtained an enormous of data from River City, including information about River City's IP address infrastructure. In addition to IP address linking River City to Liberty Lake, Washington and Spokane,

Washington via River City's ISPs, TierPoint and Cutting Edge Communications, Inc., the data itself was rife with references to Washington.

30. The publication of River City's IP address infrastructure also allowed Spamhaus to immediately blacklist River City's entire infrastructure, which effectively prevented River City from conducting business.

31. Ragan and Vickery also referenced Spamhaus listings for River City and River City's associates—these listings all give clear indications that River City and its principals live in Washington:

The Effects of the Media Campaign

32. As a direct result of Ragan's and Vickery's articles, River City lost access to the internet because Spamhaus—in collaboration with Ragan and Vickery—blacklisted numerous IP address blocks used by TierPoint and Cutting Edge Communications, Inc., which could not continue operating while blacklisted by Spamhaus. TierPoint's and Cutting Edge Communications' only recourse with

Spamhaus was to kick River City off its network, which prompted Spamhaus to delist TierPoint's and Cutting Edge Communications' IP address blocks, thereby restoring useful internet access.

33. River City lost its office lease because its offices were located in TierPoint's facility, which, without internet access, became useless to River City.

34. Spamhaus also blacklisted several domain registrars affiliated with River City on suspicion of "illegal spamming" based on Ragan's article.

35. All of the above eroded River City's ability to function and resulted in a near-cessation of business activity.

36. Because of the loss of income and business resulting from the cyberattack and Ragan and Vickery articles, River City had to lay off fourteen (14) employees and direct contractors and close down four (4) businesses, which in turn caused three (3) additional businesses to be shut down as well.

//

//

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

I declare under penalty of perjury that the foregoing is true and correct.

Executed on May 5, 2017.

Mark Ferris

NEWMAN DU WORS LLP

2101 Fourth Avenue, Suite 1500
Seattle, Washington 98121
(206) 274-2800

CERTIFICATE OF SERVICE

I hereby certify that on May 5, 2017, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system, which will send a notification of filing (NEF) to the following:

Attorneys for Defendants International Data Group, Inc., CXO Media, Inc. and Steve Ragan

Kevin J. Curtis
WINSTON & CASHATT, LAWYERS, a Professional Service Corporation
601 W. Riverside, Ste. 1900
Spokane, WA 99201
kjc@winstoncashatt.com

Charles L. Babcock
William J. Stowe
Jackson Walker L.L.P.
1401 McKinney Street, Suite 1900
Houston, TX 77010
cbabcock@jw.com
wstowe@jw.com

Attorneys for Defendant Chris Vickery

Aaron Rocke
101 Yesler Way, Suite 603
Seattle, WA 98104
aaron@rockelaw.com

Additionally, I caused true and correct copies of the foregoing to be served via first-class U.S. Mail, postage prepaid, with a courtesy copy by email to:

Attorneys for Kromtech Alliance Corp.
Matthew D. Brown
Cooley LLP
101 California Street, 5th Floor
San Francisco, CA 94111
brownmd@cooley.com

I declare under penalty of perjury that the foregoing is true and correct.

s/ Rachel Horvitz
Rachel Horvitz
Paralegal